Enhancing Correlation Electromagnetic Attack Using Planar Near-Field Cartography

Denis Réal
CELAR - IETR
35170 Bruz, France
denis.real@dga.defense.gouv.fr

Frédéric Valette
CELAR
35170 Bruz, France
frederic.valette@dga.defense.gouv.fr

Mhamed Drissi
IETR
35043 Rennes, France
Mhamed.Drissi@insa-rennes.fr

Abstract

In the field of the Side Channel Analysis (SCA), the electromagnetic radiation of a cryptographic device is the richest source of information. Indeed, it permits to be more accurate by positioning smartly the EM probe near a given logic, filtering the signal that is not useful regarding a given attack. But this advantage can become easily a drawback if the attacker is unable to position her probe onto the device. Our contribution consists in giving an accurate method detecting an hot spot onto the device, i.e. the position where a correlation electromagnetic attack (CEMA) should be the most successful. This strategy is based on an indicator evaluated during a cartography. Its performance has been tested on an hardware AES implemented on an Altera Stratix II.

1 Introduction

1.1 The side channel leakage

Whatever be the logical robustness of a cryptographic algorithm, some activity prints of its implementation may filter through. Power consumption, electromagnetic radiations, computation time... are indirect but useful informations that threaten secrets, as it has been shown by Kocher and al with the Differential Power Attack (DPA) [2]. An improvement of this attack is the Correlation Power Attack (CPA [1]): taking into account the influence of the noise is its main interest. It directly leads to a smaller number of measurements. The Electromagnetic radiation is the highest information leakage [6, 4]. Furthermore, it offers many practical advantages: no special requirement is needed for its use. The signal is also not only time-variable as the power consumption but is also space-variable: the electromagnetic signal depends on the probe position.

1.2 Classical strategy for hot spot search

The EM probe size is usually small in comparison with the device one. Locating an hot spot where one’s should position her probe is then an important part of the profiling stage of an attack. Customary, a position is assumed to be interesting for the SCA when the algorithm execution can be observed, i.e., when the signal is high compared to the noise level [5]. A by-hand search can be enough for localizing area of interest. But we can doubt that this is the smartest or the most efficient way of finding what we will call hot spots : points where the CEMA needs the less messages to succeed.

1.3 Our contribution

CEMA attacks family aims to exploit the leakage of only one logical object. Then, a high SNR for a given position does not induce a high leakage of the target object. In this article, we define a new indicator based on cryptographic and electromagnetic properties while SNR indicators are purely electromagnetic. This indicator is referred as the Sbox maximal difference indicator. In order to compare results between these various indicators, we have completed EM cartographies with SNR, Sbox energy and CEMA indicators on a hardware AES [3] implemented on an Altera Stratix using the design kit.
2 The Profiling Assumption Stage

2.1 The test bench

The signal is obtained with near field techniques. A positioning X and Y table is used to move the probe above the device. Both table and device are controlled by the same PC. In each position, all the needed experiments are performed and results stored. Then, the probe moves to the next position and a new set of measurements using the same messages is recorded. Taking into account the size of the device and the selectivity of the probe, a mapping of $20 \times 20$ is defined, which represents 400 positions for the probe. Recording all the measurements takes about 40 hours, but the CEMA cartography is the time consuming operation.

2.2 The cryptographic implementation

The targeted algorithm is an hardware AES implemented on an Altera Stratix, meaning that the cryptographic operations are done in parallel. The 16 Sboxes are computed in parallel and executed in the same clock cycle as the other operations of the same round. So the 10 rounds are executed in 10 clock cycles. This implementation is neither optimized nor protected against the SCA as our purpose is to find a method which can make the CEMA more efficient. To avoid synchronization problems, each time an encryption has been completed, a trig signal is outputted. Then, both trig signal and EM signal are recorded: the trig signal is used for time synchronization while the EM signal is used as the source of information.

3 The Various Indicators

In this section, 4 indicators which are usually used or well suitable to find the hot spots of the device are defined and their interest are detailed.

3.1 The signal to noise indicator

The usual strategy used to find the hottest spot of a device is to identify where the leakage due to the encryption is the highest. This is done by comparing an EM trace recorded during the encryption with an other one recorded when no encryption occurs. According to [4] this should give an information on the position of the algorithm on the device. This indicator can be constructed in two ways:

A first approximation consists in taking the maximum of each trace and to compare the ratio between the noise and the interesting trace. The influence of the encryption and of the noise can be estimated more sharply using 3 measurements, one for the encryption and two for the noise. This defines the indicator $SNI_{MAX}$ as:

$$SNI_{MAX} = \frac{\text{MAX}_0^T (|\Gamma_{AES} - \Gamma_{noise}|)}{\text{MAX}_0^T (|\Gamma_{noise2} - \Gamma_{noise}|)}$$  \hspace{1cm} (1)

On Fig. 1.1, the AES execution and its 10 rounds can clearly be observed: the signal level increases during the encryption.

The recorded trace on Fig. 1.2 does not permit to observe any difference due to the encryption. Then the $SNI_{MAX}$ is higher in position (0, 0) than in position (3, 17).

The second possibility is to consider the signal more globally. Instead of just considering the signal at one instant, the indicator can be time-integrated. This strategy may be more suitable as this integration can represent the consumption of the encryption. $SNI_T$ can be written as: to consider the signal more globally. Instead of just considering the signal at one instant, the indicator can be time-integrated. This strategy may be more suitable as this integration can represent the consumption of the encryption. $SNI_T$ can be written as:

$$SNI_T = \frac{\int_0^T (|\Gamma_{AES} - \Gamma_{noise}|)}{\int_0^T (|\Gamma_{noise2} - \Gamma_{noise}|)}$$ \hspace{1cm} (2)

Both techniques are considered and compared below as it takes only few minutes to perform a cartography on.

3.2 The Sbox maximal difference indicator

As our goal is to perform a CEMA on a specific object (say for example a Sbox Output), it might be useful to find the position where the EM signal is the most correlated with it. For a given logical object, there are two kinds of noise on a side channel signal. The device activity noise is already taken into account in the previous indicator family.
Just remains the logical noise due to the others bits activity. So in this second family of indicator, we try to minimized the effect of the other phenomena occurring during the encryption and reveal the effect of the targeted Sbox. More precisely, we try to see if the hot spots are different from an Sbox to another one.

The targeted logical object is the output of the Sbox \(i\) with \(0 \leq i < 16\). The main source of logical noise is assumed to be the other Sboxes activity. Our strategy consists then in choosing plaintexts with a variable part and a fixed part. The variable part aims to stimulate the activity of the \(i^{th}\) Sbox while the activity of the other Sboxes is kept constant thanks to the plaintext fixed part. Studying the EM signal with these constraints on the plaintexts permits to estimate the activity of the Sbox \(i\). If the attacker does the same procedure on all the Sboxes, she should be able to correlate this Sbox distinguisher with the probe position.

As the secret key is assumed unknown, specific messages cannot be chosen for maximizing the difference on the Sbox output. Anyway, but we are able to choose for each Sbox two messages which lead to a difference only in the output of the chosen Sbox. For example with the messages \(M_1 = 0x00\ldots 0.00\) and \(M_2 = 0xFF00\ldots 0.00\), only the \(1^{st}\) Sbox is activated. The difference between the measurements with the two messages should represent the influence of the Sbox. As for the first indicator, both the maximum or also the integrated signal during the \(1^{st}\) round are considered.

So we can defined the Maximal Difference Indicator \((MDI_{MAX})\) as:

\[
MDI_{MAX} = \frac{\text{MAX}_0^T (|\Gamma_{M_1} - \Gamma_{M_2}|)}{\text{MAX}_0^T (|\Gamma_{M_1'} - \Gamma_{M_2'}|)}
\] (3)

Fig. 2 shows the difference due to different encryptions. This difference is much bigger than the noise level at the considered position.

The second possibility is to consider the signal more globally. Instead of just considering the signal at one instant, the indicator can be time integrated. This technique may be more suitable as this integration can represent the consumption of the encryption. \(MDI_T\) can be written as:

\[
MDI_T = \frac{\int_0^T (|\Gamma_{M_1} - \Gamma_{M_2}|)}{\int_0^T (|\Gamma_{M_1'} - \Gamma_{M_2'}|)}
\] (4)

These indicators can be built for each Sbox with only 17 messages and it costs only a few minutes to perform a complete cartography on the device.

### 3.3 The CEMA indicator

The last indicator is linked to the CEMA, more precisely to the number of messages needed to perform a CEMA. To build it, the whole attack must be performed on each point. So 10000 random messages are chosen and a CEMA is done on each point by sending the same group of messages in every position. This operation is very long and takes more than one day but is necessary to define which of the previous indicator is the most relevant. This indicator can be represented in two ways: we can define the minimal number of messages which gives the right result for the key or we can defined for a fixed number of the messages the ratio of the maximum value of the CEMA peak of the right key and the mean of the maximum value of the CEMA peak for the other value of the key.

### 4 Cartography

In this part, the result of the indicators’ cartography are compared with the CEMA results. We also compare the image given by the routing software of the FPGA to see if the most interesting points are linked with the real position of the implementation. For the cartography, a white point means that the indicator has its lowest value on this position while a black point means that the indicator has its highest value on the position. The darkness of the point is proportional to the value of the indicator.

#### 4.1 The image of the Stratix floorplan AES

The image presented in Fig. 3 shows how the various blocks of our design are placed in the FPGA and which wires or cells are used. 3 different blocks exist: the RS232 interface (referred as RS232), the key scheduling block (KS) and the round function block (RF). The various cartographies built using the indicators should be correlated with this design.
4.2 The signal to noise cartography

The results of the cartography in Fig. 4 shows that the SNI identifies the key scheduling block more than the round function block.

A cartography on \( SNI_T \) shows it is less precise than the \( SNI_{MAX} \). This is quite natural as it takes more points and can then means the effect of the noise.

4.3 The maximal difference indicator cartography

The \( MDIs \) results are much better than the \( SNIs \) ones. The interesting areas are smaller than the areas obtained with the \( SNIs \). Furthermore, they are located on the round function block.

The cartography using the whole period of the first round and not only the maximum, seems more precise. It is illustrated on Fig. 5 for the Sbox 0. This is mainly due to the fact that the execution of a round is not instantaneous but requires a small amount of time for gate and wire propagation.

We can also observed on the Fig. 6 that the interesting areas are different for each Sbox we target. But it seems difficult to extract a precise information on the location of each Sbox. As previously, \( MDIs \) are interesting as they give information on the position where the most significant correlation between the EM emanation and the Sbox behavior is.
4.4 The CEMA cartography

Finally, the CEMA cartography using the minimum number of messages to guess the right key is performed.

Its is illustrated on Fig. 7 for the Sbox 0 This cartography match with the MDI cartography (the MDIT is more accurate) and not with the SNI cartography. The amount of needed messages varies from 1700 for the most interesting point to 5000 for the least significant. So we proved that, using the MDI, an attacker can reduce the number of needed messages (in our case by a factor 3). This gain is quite interesting but smaller than what we can expect regarding the values of the MDIs. Indeed, the CEMA we performed is not able to extract all the information contained in EM measurements on the points revealed by the MDI cartography. This is mainly due to the fact that the hamming distance we used for the CEMA may be not representative of the component behavior and may be less suitable for hardware than for software implementation.

But something is more surprising: the CEMA works everywhere. More precisely, wherever the probe is set, the CEMA succeed with less than 5000 messages. Even in position where no correlation can be found between the AES execution and the EM emanation, the CEMA succeeds. For example, in the position of the curve on Fig. 1.2, where we are not able to see any difference between the AES execution and the noise, the CEMA needs only 5000 messages to succeed. This proves the efficiency of the CEMA. Furthermore, as illustrated on Fig. 8, the success rate of the CEMA is continuous: the number of message needed for mounting a CEMA is quite the same for two close positions.

5 Conclusion

With the various cartographies that have been made, two important points have been discovered.

The first point is that we have found an indicator, easy to evaluate, which can improve a CEMA by reducing the number of needed messages. The indicator reveals hot spots: specific points where an attacker have to put its probe in order to minimize the number of messages. This technique may also be applicable with much accuracy for Simple Electromagnetic Attack (SEMA) and Templates Attacks (TA).

The second important point is that once an attacker have a precise trigger to synchronize its measurement, she can perform a successful CEMA with a very small amount of curves, even if she is not able to distinguish the AES execution. Moreover, the success rate of the CEMA is continuous with the probe position. All these measurements suggest a question: is it possible to optimize the CEMA by a better understanding of the EM-emanation of an AES hardware implementation?

References


